Date of acceptance : 23/01/2015

Published ID	:	C-362/14
Document number	:	22
Register number	:	977578
Date of lodgment	:	10/11/2014
Date of entry in the register	:	11/11/2014
Type of document	:	Observations
	:	Document
Lodgment reference	:	DC33664
File number	:	1
Person lodging document	:	McGarr Edward Digital Rights Ireland

IN THE COURT OF JUSTICE

OF THE EUROPEAN UNION

Case C-362/14

MAXIMILIAN SCHREMS

Plaintiff

-and-

DATA PROTECTION COMMISSIONER

Defendant

And

DIGITAL RIGHTS IRELAND LIMITED

Notice Party

WRITTEN OBSERVATIONS OF DIGITAL RIGHTS IRELAND LIMITED

Submitted by McGarr Solicitors, 12 City Gate, Lower Bridge Street Dublin 8 acting as agent for the Notice Party, Digital Rights Ireland Limited, assisted by Mr. Fergal Crehan, Barrister of the Bar of Ireland.

Service of documents may also be made by fax or by email:
Fax: (353) 1 6351580
Email: info@mcgarrsolicitors.ie

These are the written observations of Digital Rights Ireland Limited in the proceedings that are the subject of the present reference. They are submitted pursuant to the second paragraph of Article 23 of the Protocol on the Statute of the Court of Justice of the European Union

Introduction

1. These submissions are made by and on behalf of Digital Rights Ireland Limited (DRI), in its capacity as *amicus curiae* in the within proceedings.

2. DRI was founded in 2005 and is a not-for-profit undertaking devoted to defending civil, human and legal rights in a digital age. It seeks to inform and educate members of the public regarding their rights in the information society and where possible to vindicate and assist in vindicating those rights.

3. DRI is a member of the European Digital Rights Initiative – EDRI, and also works with other civil rights groups such as the Irish Council for Civil Liberties, the UK-based Privacy International and the US-based Electronic Frontier Foundation.

4. DRI was the Plaintiff in a case heard before the High Court of Ireland, in a case entitled Digital Rights Ireland Limited v Minister for Communication and Ors[1]. In that matter a number of matters were referred to the Court of Justice of the European Union for reference, Mr Justice McKechnie of the High Court finding that the Applicant was a "sincere and serious litigant" and that in the context of that case it was appropriate to grant the Applicant the ability to advance arguments on behalf of citizens in general, in the nature of an *actio popularis.*

5. In the subsequent reference to the Court of Justice of the European Union, it was held that the Directive the subject of the reference, 2006/24/EC (the "Data Retention Directive") was invalid having regard to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

6. DRI was joined in the matter of Schrems v Data Protection Commissioner as *amicus curiae* by order of Mr. Justice Hogan of the Irish High Court of 16th July, 2014. DRI maintains a strong interest in those proceedings owing to the fact that they were the first consideration by a Court of a member state of the European Union of the effect of Commission Decision 2000/520/EC of 26 July 2000 ("the Decision") vis-á-vis the provisions of European Union law, and in particular with regard to Articles 7 & 8 of the Charter of Fundamental Rights of the European Union. The said decision affects the personal data of every citizen of the European Union.

1 [2010] IEHC 221

7. The High Court of Ireland refers the following questions to the Court of Justice:

   "1. Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC)) having regard to Article 7, Article 8 and Article 47 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?

   2. Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

8. Our answer, in short, is that the Charter of Fundamental Rights of the European Union requires the office holder (being, in the instant case, the Data Protection Commissioner of Ireland) to conduct his own investigation in light of certain developments, specifically the coming into force of the EU Charter, and those matters subject of the Snowden revelations. Insofar as he is forbidden from conducting such an investigation, the Decision, which thus forbids him, is invalid under EU law.

9. It is the submission of DRI, which will be elaborated upon in this document, that the Charter of Fundamental Rights and the General Principles of European Union law require that the Decision provide for independent supervision of the operation of the Safe Harbour system in order to ensure that it respects, in its operation, the Fundamental Rights of the EU citizen. Only insofar as the Decision fulfils this requirement is it valid under the Charter and the General Principles. Insofar as (and this is the submission of Digital Rights Ireland) the Decision fails to so provide, it is invalid under community law.

10. Further, irrespective of the safeguards which may or may not be built into the Safe Harbour system, it is clear that it does not at present operate as initially envisaged, and may never have. The factual developments regarding the access to Safe Harbour data which has been afforded to US law enforcement agencies present an entirely different climate to that which was assumed at the time of the making of the Decision on adequacy. Accordingly, and in the absence of any renegotiation of the Agreement, the operation of Safe Harbour, as a simple matter of fact, is in breach of the Charter of Fundamental Rights and the general principles of EU law, in particular Articles 7 and 8, but also of the rights to Freedom of Expression and to Freedom of Association and Assembly, as provided for, *inter alia*, by Articles 11 and 12 of the Charter.

11. DRI submits that the "factual developments" referred to in the question of the High Court can be classed into two broad categories:

    A. Recent Developments in the law of the European Union, specifically, the coming into force of the EU Charter of Human Rights, and the subsequent case law of the Court of Justice of the European Union.
    B. Recent revelations by Edward Snowden regarding the degree to which American law enforcement services have been granted access to the data of European Union citizens. (see the Annex to these Written Observations for the documents which have come into the public domain through Edward Snowden's actions)

12. These two elements must be considered in detail in order to fully answer the question referred by the Irish High Court. However, as a preliminary matter, we must consider the text of the Decision, and the Directive on foot of which it was made, in order to consider whether it is capable of an interpretation which allows a regulator to undertake an independent investigation.

Applicable Law Relating to the within proceedings

Whether the Commission Decision on Adequacy Precludes Further Investigation

13. Section 11(1) of the Data Protection Acts 1988-2003 provides that

    "*The transfer of personal data by a data controller to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer*"

14. Section 11(2) goes on to set out the manner in which such adequacy of protection is to be determined. Of relevance to the proceedings herein is section 11(2)(a) which states:

    "(*2) (a) Where in any proceedings under this Act a question arises-*

    whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area to which personal data are to be transferred,

    and

    a Community finding has been made in relation to transfers of the kind in question, the question shall be determined in accordance with that finding."

15. A “Community finding” is then defined thus by Section 11(2)(b)

“In paragraph (a) of this subsection “Community finding” means a finding of the European Commission made for the purposes of paragraph (4) or (6) of Article 25 of the Directive under the procedure provided for in Article 31(2) of the Directive in relation to whether the adequate level of protection specified in subsection (1) of this section is ensured by a country or territory outside the European Economic Area”

16. “The Directive” is defined by s. 1(1) as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (“the Data Protection Directive”). Article 25(6) of the Directive provides that:

“*The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitment it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of private lives and basic freedoms and rights of individuals.*

Member States shall take the measures necessary to comply with the Commission’s decision.”

17. Such a decision, Decision 2000/520/EC (“the Decision”) was in fact made, on the 25th August, 2000. The Decision provides, at Article 1, that

“1. For the purposes of Article 25(2) of Directive 95/46/EC, for all the activities falling within the scope of that Directive, the "Safe Harbor Privacy Principles" (hereinafter "the Principles"), as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States, having regard to the following documents issued by the US Department of Commerce:

a. *the safe harbour enforcement overview set out in Annex III;*

b. *a memorandum on damages for breaches of privacy and explicit authorisations in US law set out in Annex IV;*

c. *a letter from the Federal Trade Commission set out in Annex V;*

d. *a letter from the US Department of Transportation set out in Annex VI.*

2. In relation to each transfer of data the following conditions shall be met:

a. the organisation receiving the data has unambiguously and publicly disclosed its commitment to comply with the Principles implemented in accordance with the FAQs; and

b. the organisation is subject to the statutory powers of a government body in the United States listed in Annex VII to this Decision which is empowered to investigate complaints and to obtain relief against unfair or deceptive practices as well as redress for individuals, irrespective of their country of residence or nationality, in case of non-compliance with the Principles implemented in accordance with the FAQs.

c. The conditions set out in paragraph 2 are considered to be met for each organisation that self-certifies its adherence to the Principles implemented in accordance with the FAQs from the date on which the organisation notifies to the US Department of Commerce (or its designee) the public disclosure of the commitment referred to in paragraph 2(a) and the identity of the government body referred to in paragraph 2(b).

18. The purported effect of this article is to allow data transfers to the United States where the organisation in question self-certifies its adherence to the Safe Harbour Principles. Such self-certification, via the legislation set out above, has the effect of requiring the Data Protection Commissioner, under Section 11(2) of the Data Protection Acts, to conclude that the self-certifying organisation has provided an "adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects".

19. A textual analysis of the Decision itself will allow the Court to consider whether the Decision can be interpreted as allowing independent investigations, or whether, even on the most generous construction, it does not, and is accordingly invalid under Article 8 of the Charter and specifically 8.3.

20. Recital 8 of the Decision provides

"*In the interests of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify in this Decision the exceptional circumstances in which the suspension of specific data flows should be justified, notwithstanding the finding of adequate protection."*

21. Such provision for suspension of specific data flows in exceptional circumstances are provided for at Article 3 of the Decision:

"*1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to an organisation that has self-certified its adherence to the Principles implemented in accordance with the FAQs in order to protect individuals with regard to the processing of their personal data in cases where:*

(a) the government body in the United States referred to in Annex VII to this Decision or an independent recourse mechanism within the

meaning of letter (a) of the Enforcement Principle set out in Annex I to this Decision has determined that the organisation is violating the Principles implemented in accordance with the FAQs; or

(b) there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

The suspension shall cease as soon as compliance with the Principles implemented in accordance with the FAQs is assured and the competent authorities concerned in the Community are notified thereof."

22. We must therefore consider whether an ascertainment, under Article 3.1(b), constitutes an "investigation" of the type envisaged by the High Court of Ireland in its referral question.

23. It is clear from the text of the Decision that what is envisaged is an investigation by a domestic Data Protection regulator of specific cases in individual organisations, in cases where enforcement provided under the Decision is failing to operate adequately. What is not provided for is a broader assessment of the adequacy of the protections provided by the law and practices of a third country. This is clear not only from recital 8, but also from Article 3.1(b). It is further noted that Article 3.1 envisages an end to a suspension once compliance is assured.

24. The High Court, in its referral, seeks guidance on whether a domestic Data Protection Regulator may, "in light of factual developments" since the time of the Commission Decision, conduct enquiries as to the adequacy of "the law and practices" of a third country, "which, it is claimed, do not contain adequate protections for the data subject".

25. It is clear, therefore, that the kind of enquiry envisaged by the High Court of Ireland is one which can potentially find otherwise than the finding of adequacy contained in Decision 2000/520/EC. In respect of Article 3.1(b) the Communication of the Commission (2013) 847 says

> *"Under the Decision, the EU national data protection authorities (DPAs) have the right to suspend data transfers to Safe Harbour certified companies in specific cases. The Commission is not aware of any cases of suspension by a national data protection authority since the establishment of Safe Harbour in 2000. Independently of the powers they enjoy under the Safe Harbour Decision, EU national data protection authorities are competent to intervene, including in the case of international transfers, in order to ensure compliance with the general principles of data protection set forth in the 1995 Data Protection Directive."*

26. The Commission however emphasises in its communication that aside from such temporary suspensions of certain individual transfers as are envisaged in Article 3, "**it is the competence of the commission**" (bold in original) to suspend the Decision itself. This, it interestingly notes,

> *"is notably foreseen if there is a systemic failure on the US side, for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role, or if the level of protection provided by the Safe Harbour Principles is overtaken by the requirements of US legislation."*

27. Further, it is to be noted that Article 26.6ii of Directive 95/46 states that "*member States shall take the measures necessary to comply with the Commission's decision.*". This appears to offer no discretion to Member states that have doubts as to the factual accuracy of the Decision regarding adequacy, as opposed to doubts as to the compliance of certain specific organisations with the Safe Harbour Principles. Accordingly, in order to be valid under the Charter, the Decision ought to provide such discretion in its own text. As set out above, it fails to do so.

28. In addition (and more particularly relevantly to the reference herein), the decision only permits suspension of data flows "under existing legislation". In fact, not all member states provided, under their data protection legislation existing at the time of the making of the Decision, for such suspensions. Indeed, many still do not do so. Accordingly, the Decision fails to provide, *across the EU as a whole*, for any investigation into adequacy of protection of transferred data. Ireland's Data Protection Acts provide for no such suspension, but rather treat the Decision as creating an irrebuttable presumption that the laws and practices of a third country provide adequate protection.

29. Accordingly, the answer to the question of Hogan J must be that the Office holder in the referral herein *is* absolutely bound by the Community finding regarding the adequacy of protections for the data subjects contained in the laws and practices of another third country (in this case, the United States of America), and may not conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published.

30. However, the matter does not end there, as it follows from that conclusion that the Decision itself must be invalid in that it permits the creation of an irrebuttable

presumption regarding the protection afforded to fundamental rights in certain third countries. In NS and Ors[2], the Court held that European Union law precludes the application of a conclusive presumption that a member state observes the Fundamental Rights of the European Union. In a particularly relevant passage it added that the same must apply to a finding regarding third countries:

"It follows from all of the foregoing considerations that, as stated by the Advocate General in paragraph 131 of her Opinion, an application of Regulation No 343/2003 on the basis of the conclusive presumption that the asylum seeker's fundamental rights will be observed in the Member State primarily responsible for his application is incompatible with the duty of the Member States to interpret and apply Regulation No 343/2003 in a manner consistent with fundamental rights.

In addition, as stated by N.S., were Regulation No 343/2003 to require a conclusive presumption of compliance with fundamental rights, it could itself be regarded as undermining the safeguards which are intended to ensure compliance with fundamental rights by the European Union and its Member States.

That would be the case, inter alia, with regard to a provision which laid down that certain States are 'safe countries' with regard to compliance with fundamental rights, if that provision had to be interpreted as constituting a conclusive presumption, not admitting of any evidence to the contrary."

31. In addition, by allowing for a suspension data flows only by member states who had such power under existing national legislation, or by not explicitly granting such a power to the regulators of all members states, the Decision fails to provide equal access to a remedy to citizens across the member states of the EU. Without prejudice to the foregoing submissions regarding the scope of this power to suspend data flows, the Decision fails to provide for control of compliance with the right to data protection by an independent authority, as required by Article 8.3 of the Charter (considered further below).

The Rights to Privacy and Data Protection

The General Principles of EU Law

32. Article 2 of the Treaty on the European Union provides that the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. The plaintiff contends that the measures sanctioned by the Decision of 2000 are such as to be contrary to the provisions of Article 2.

33. Article 6 of the Treaty of the European Union provides

"Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."

34. The UN Universal Declaration of Human Rights provides at Article 12:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"

35. The International Covenant on Civil and Political Rights (ICCPR) provides, at Article 17:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks."

36. These documents, in so far as they represent the shared values of all European Union member states[3], constitute sources of the General Principles of the law of the European Union. In *Orkem v Commission*[4] and other cases, the ICCPR was expressly cited as a source of the General Principles of Community law.

37. *Bunreacht na hÉireann*, the Constitution of Ireland, is, as provided by Article 6 TEU, a source of the General Principles. It provides, at Article 40.5

"The dwelling of every citizen is inviolable and shall not be forcibly entered save in accordance with law."

3 See para 35, C-540/03 *Parliament v Commission*

4 Case 374/87

38. In *Schrems v Data Protection Commissioner*[5], the judgment of the High Court of Ireland in which the referral herein was made, Hogan J considered this provision as it relates to privacy and data protection, and in light of the Constututional traditions of other member states:

> *"...the accessing by State authorities of private communications generated within the home – whether this involves the accessing of telephone calls, internet use or private mail – also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution. As it happens, by one of those accidents of legal history, these very same words are also contained in Article 13(1) of the German Basic Law ("inviolability of the dwelling") ("unverletzlichkeit der Wohnung"). It is, accordingly, of interest that the German Constitutional Court has held that the accessing by state authorities of otherwise private communications within the home also engages that more or less identically worded guarantee of inviolability of the dwelling which is contained in Article 13(1) of the Basic Law. Indeed that Court went further and found that legislation providing for the interception and surveillance of communications partly unconstitutional because it provided for a disproportionate interference without adequate safeguards with that very guarantee of inviolability of the dwelling in Article 13(1) of the Basic Law: see Anti-Terrorism Database Law decision (1 B v R 1215/07)(April 24, 2013) at paras. 93 et seq.*
>
> *49. Naturally, the mere fact that these rights are thus engaged does not necessarily mean that the interception of communications by State authorities is necessarily or always unlawful. The Preamble to the Constitution envisages a "true social order" where the "dignity and freedom of the individual may be assured", so that both liberty and security are valued. Provided appropriate safeguards are in place, it would have to be acknowledged that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of State security. It is accordingly plain that legislation of this general kind serves important – indeed, vital and indispensable - State goals and interests: cf. by analogy the decision of the German Constitutional Court in the Anti-Terrorism Database case (at paras. 106, 131 and 133, passim) and the comments of the Court of Justice in Case C-293/12 Digital Rights Ireland Ltd. [2014] E.C.R. I-000 at paras. 42-44.*

[5] [2014] IEHC 310

50. The importance of these rights is such nonetheless that the interference with these privacy interests must be in a manner provided for by law and any such interference must also be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home. While the use of the term "inviolable" in respect of the dwelling in Article 40.5 does not literally mean what it says, the reference to inviolability in this context nonetheless conveys that the home enjoys the highest level of protection which might reasonably be afforded in a democratic society: see, e.g., Wicklow County Council v. Fortune (No.1) [2012] IEHC 406.

51. By safeguarding the inviolability of the dwelling, Article 40.5 provides yet a further example of a leitmotif which suffuses the entire constitutional order, namely, that the State exists to serve the individual and society and not the other way around.

52. In this regard, it is very difficult to see how the mass and undifferentiated accessing by State authorities of personal data generated perhaps especially within the home – such as e-mails, text messages, internet usage and telephone calls – would pass any proportionality test or could survive constitutional scrutiny on this ground alone. The potential for abuse in such cases would be enormous and might even give rise to the possibility that no facet of private or domestic life within the home would be immune from potential State scrutiny and observation.

53. Such a state of affairs – with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker - would be totally at odds with the basic premises and fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2); the inviolability of the dwelling (Article 40.5) and protection of family life (Article 41). As Hardiman J. observed in The People v. O'Brien [2012] IECCA 68, Article 40.5

1. *"...presupposes that in a free society the dwelling is set apart as a place of repose from the cares of the world. In so doing, Article 40.5 complements and re-inforces other constitutional guarantees and values, such as assuring the dignity of the individual (as per the Preamble to the Constitution), the protection of the person (Article 40.3.2), the protection of family life (Article 41) and the education and protection of children (Article 42). Article 40.5 thereby assures the citizen that his or her privacy, person and security will be protected against all comers, save in the exceptional circumstances presupposed by the saver to this guarantee."*

54. One might accordingly ask how the dwelling could in truth be a "place of repose from the cares of the world" if, for example, the occupants of the dwelling could not send an email or write a letter or even conduct a telephone conversation if they could not be assured that they would not be subjected to the prospect of general or casual State surveillance of such communications on a mass and undifferentiated basis.

55. That general protection for privacy, person and security in Article 40.5 would thus be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversations and communications which take place within the home. For such interception of communications of this nature to be constitutionally valid, it would, accordingly, be necessary to demonstrate that this interception of communications and the surveillance of individuals or groups of individuals was objectively justified in the interests of the suppression of crime and national security and, further, that any such interception was attended by appropriate and verifiable safeguards."

The European Convention on Human Rights

39. Article 6.1 of the Treaty on the European Union provides that the Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted at Strasbourg, on 12 December 2007, which have the same legal value as the Treaties.

40. Article 6.2 of the Treaty on the European Union provides that the European Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Article 6.3 of the TEU provides that fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, are to constitute general principles of the Union's law.

41. The European Convention for the Protection of Human Rights and Fundamental Freedoms, a source of the General Principles of European Union Law, provides (*inter alia*, and subject to certain limitations) at Article 8

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."*

42. Digital Rights Ireland asserts that the Decision, insofar as it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to personal data by foreign law enforcement authorities, is a direct invasion of the privacy of all

electronic correspondence, and consequently an invasion of the privacy of legal and natural persons, and of the private and family life of citizens of the Member States of the European Union.

43. In *Uzun v Germany*[6], the European Court of Human Rights (ECtHR) discussed its jurisprudence in the area:

> *"The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 protects, inter alia, a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see P.G. and J.H. v. the United Kingdom, no. 44787/98, § 56, ECHR 2001-IX; Peck v. the United Kingdom, no. 44647/98, § 57, ECHR 2003-I; and Perry v. the United Kingdom, no. 63737/00, § 36, ECHR 2003-IX (extracts)).*
>
> *There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor (see Perry, cited above, § 37). A person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character (see also Herbecq and the Association "Ligue des droits de l'homme" v. Belgium, nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, Decisions and Reports (DR) 92-B, p. 92, concerning the use of photographic equipment which does not involve the recording of the visual data obtained). Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain (see P.G. and*

[6] No. 35623/05 §§43-46, ECHR 2010

J.H. v. the United Kingdom, cited above, § 57; Peck, cited above, §§ 58-59; and Perry, cited above, § 38).

Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable.

Thus, the Court has considered that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V; P.G. and J.H. v. the United Kingdom, cited above, § 57; Peck, cited above, § 59; and Perry, cited above, § 38; compare also Amann v. Switzerland [GC], no. 27798/95, §§ 65-67, ECHR 2000-II, where the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted). The Court has also referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force – inter alia for Germany – on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual"

44. In *S & Marper v United Kingdom*[7], retention of data relating to DNA and cell samples, and fingerprints was held to be a violation of Article 8 of the ECHR. The

[7] Nos 30562/04 and 30566/04, §67, ECHR 2008

Plaintiff notes the Court held that this was so irrespective of the use to which the data was put:

> "*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see Leander v. Sweden, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding*"

45. Insofar as the accessing of data transferred under the differs from that pertaining in *Marper*, the Plaintiff submits that the accessing of electronic communications is more intrusive. While DNA and cellular information is by its nature highly personal, it relates less to the private and family lives of individuals than do electronic communications. Electronic communications can build up a detailed picture of an individual's habits, relationships, and even beliefs. DNA, cellular or fingerprint data stand alone, and do not, of themselves, provide any such account of an individual's personal and family life.

46. Where the data retention in *Marper* was limited to persons suspected of criminal activity, the transfer of data provided for by the Decision applies to practically every citizen of the European Union. Further, where the proportionality of the data processing in *Marper* was measured against the aim of prevention and investigation of crime, no such countervailing concern can be cited with regard to the Decision of 2000.

47. In *Z v Finland*[8] the ECtHR, in holding that the publication of HIV test result were a breach of Article 8 ECHR, stated

> *"In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention"*

[8] No. 22009/93 ECHR 1997

48. In *Niemietz v Germany*[9], the Court, in holding that a search of correspondence in a law office was in breach of Article 8, stated

> *"The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."*

49. In *Amann v Switzerland*[10], in holding that Article 8 was breached by interceptions of telephone calls and the creation and storage of a card recording details from these calls, the Court made an explicit link between the rights to privacy and to Data Protection, holding:

> *"The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, p. 22, § 48).*
>
> *It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life" (see the Niemietz v. Germany judgment of 16 December 1992, Series A no. 251-B, pp. 33-34, § 29, and the Halford judgment cited above, pp. 1015-16, § 42).*
>
> *That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2)."*

9 No. 13710/88 ECHR 1992

10 No. 27798/95 ECHR 2000

50. In *S & Marper*, considered above, the Court held that "in accordance with the law" means, *inter alia*, that

> *"The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct."*

51. This question of foreseeability was further considered in *Weber & Savaria v Germany*[11], the Court holding:

> *"93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, inter alia, Leander, cited above, p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, Malone, cited above, p. 32, § 67; Huvig, cited above, pp. 54-55, § 29; and Rotaru, cited above, § 55). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see Kopp v. Switzerland, judgment of 25 March 1998, Reports 1998-II, pp. 542-43, § 72, and Valenzuela Contreras v. Spain, judgment of 30 July 1998, Reports 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see Malone, ibid.; Kopp, cited above, p. 541, § 64; Huvig, cited above, pp. 54-55, § 29; and Valenzuela Contreras, ibid.).*
>
> *94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any*

[11] No 54934/00 ECHR 2006

such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, Malone, cited above, pp. 32-33, § 68; Leander, cited above, p. 23, § 51; and Huvig, cited above, pp. 54-55, § 29).

95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, Huvig, cited above, p. 56, § 34; Amann, cited above, § 76; Valenzuela Contreras, cited above, pp. 1924-25, § 46; and Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003)"

52. It is the submission of Digital Rights Ireland that Safe Harbour, as it currently operates, cannot provide this necessary foreseeability, insofar as the European citizen has no way of knowing, whether, or on what basis her data has been accessed by Unites States law enforcement authorities. In particular, the minimum safeguards set out in paragraph 93 of *Weber* are absent.

The Charter of Fundamental Rights of the European Union

Articles 7 & 8

53. Article 7 of the Charter of Fundamental Rights of the European Union provides

"Everyone has the right to respect for his or her private and family life, home and communications"

54. Digital Rights Ireland asserts that the Decision, insofar as it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to personal data by foreign law enforcement authorities, infringes Article 7.

55. Article 8 of the Charter of Fundamental Rights of the European Union provides

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

56. The Plaintiff asserts that the Decision allows or, or in the alternative fails and has failed to prohibit the collection and accessing of data of legal and natural persons, without consent, and on an automatic and general basis, and therefore without specific reason or purpose.

57. Without prejudice to the generality of these submissions, it is the position of Digital Rights Ireland that the transfers the subject of the within proceedings are of a different nature to those envisaged by the Decision of 2000. At that time, open access to such data for the purposes of law enforcement or national security was not contemplated. It is a core principle of Data Protection law that data must only be processed for a specified purpose. Any change in the purpose to which transferred data is put is a new instance of data processing. In this regard, the Decision does not relate to transfers of the kind in question in the proceedings had herein.

58. In *Volker and Markus Schecke GbR v Land Hessen*[12] and *Eifer v Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung*[13], the Court held

"Article 8(1) of the Charter states that '[e]veryone has the right to the protection of personal data concerning him or her'. That fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter."

[12] C-92/09

[13] C-93/09

59. And, in declaring certain of the measures subject of the reference invalid, that

> *"institutions are obliged to balance, before disclosing information relating to a natural person, the European Union's interest in guaranteeing the transparency of its actions and the infringement of the rights recognised by Articles 7 and 8 of the Charter. No automatic priority can be conferred on the objective of transparency over the right to protection of personal data (see, to that effect, Commission v Bavarian Lager, paragraphs 75 to 79), even if important economic interests are at stake."*

60. The measures at issue in these linked cases were the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). These measures were much less intrusive into the private lives of the persons affected, and much more limited in terms of the number of people to whom they apply than the Decision the subject of the present reference.

61. On April 8 the Court of Justice of the European Union (CJEU) announced its judgment in joined cases C-293/12 and C-594/12 Digital Rights Ireland. Based on EU fundamental rights law, the Court invalidated the EU Data Retention Directive, which obliged telecommunications service providers and Internet service providers in the EU to retain telecommunications metadata and make it available to European law enforcement authorities under certain circumstances. The case illustrates the key role that the EU Charter of Fundamental Rights ("The Charter") plays in EU data protection law.

62. The Directive was struck down notwithstanding that it, like the Decision of 2000, pre-dated the coming into effect of the Charter. Indeed, at hearing, submissions on behalf of the European Commission that the Charter could have no retrospective effect were dismissed by the CJEU.

63. In Digital Rights Ireland v Ireland, the Court of Justice noted, with regard to data retained under Directive 2006/24, that

> *"even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently,*

on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article (Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert EU:C:2010:662, paragraph 47)"

64. Advocate-General Cruz Villalon, in the same case, stated

> "*The data in question, it must be emphasised once again, are not personal data in the traditional sense of the term, relating to specific information concerning the identity of individuals, but 'special' personal data, the use of which may make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity*"

65. The Applicant notes that no distinction between "metadata" and the content of communications can be made in respect of the data transferred under the Decision of 2000. Entire communications or threads of communications, from the most brief and trivial exchange on Facebook or other social media platforms to lengthy and intimate correspondence via email, are transferred, and therefore open to undifferentiated access by foreign law enforcement. Such data are more intimate again even than those at issue in the Data Retention case, being qualitative rather than quantitative. Data of the kind transferred under the Decision of 2000 are capable of showing not only who an individual *is*, but what that individual is *like*.

66. The intimacy of this data, and its significance for the rights of the individual in society is well illustrated by a detail from a recent article in the New York Review of Books:

> *"One company, Acxiom, for example, has profiles on 75 percent of all Americans, each with around five thousand individual data points that can be*

constructed and deconstructed to find, say, people who live near nuclear power plants who support Greenpeace, or practicing Muslims who own guns. It should come as no surprise that the NSA and the Departments of Defense and Homeland Security buy this material from Acxiom."[14]

67. Digital Rights Ireland notes that Axciom is on the list of Safe Harbour companies.

Freedom of Expression

68. The United Nations Universal Declaration of Human Rights, a source of the General Principles of European Union law, provides at Article 19, that

> *"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."*

69. The United Nations International Covenant on Civil and Political Rights, a source of the General Principles of European Union Law, provides at Article 19.2, that

> *"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."*

70. The European Convention for the Protection of Human Rights and Fundamental Freedoms, a source of the General Principles of European Union Law, provides (*inter alia*, and subject to certain limitations) at Article 10. that

> "*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."*

71. The Charter of Fundamental Rights of the European Union provides, at Article 11,

[14] Sue Halpern, *Partial Disclosure*, New York Review Of Books, 10th July, 2014 at 16

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

72. Digital Rights Ireland notes that in both the Charter and the ECHR, this right is explicitly stated to apply "regardless of frontiers".

73. The knowledge that one's speech is being monitored, or even potentially being monitored, gives rise to an inhibition on speech known as the "chilling effect", or, more sinisterly, the "panopticon effect". In the First Amendment jurisprudence of the United States of America, legislation resulting in a chilling effect on Free Speech has repeatedly been struck down. In *Lamont v Postmaster General*[15], for example, a statute requiring that a postal patron receiving communist political propaganda to specifically authorize the delivery was struck down as an unacceptable governmental interference in Free Speech:

"This requirement is almost certain to have a deterrent effect, especially as respects those who have sensitive positions. Their livelihood may be dependent on a security clearance. Public officials, like schoolteachers who have no tenure, might think they would invite disaster if they read what the Federal Government says contains the seeds of treason. Apart from them, any addressee is likely to feel some inhibition in sending for literature which federal officials have condemned as "communist political propaganda." The regime of this Act is at war with the "uninhibited, robust, and wide-open" debate and discussion that are contemplated by the First Amendment"

74. Digital Rights Ireland submits that insofar as it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, the Decision has such an inhibitory or "chilling"

15 381 U.S. 301 (1965)

effect on freedom of expression. In this respect the Decision infringes the right to freedom of Expression as guaranteed under European Union law.

75. The European Court of Human Rights has repeatedly emphasised that Charter Article 10 safeguards not only the substance and contents of information and ideas, but also the means of transmitting it. The press has been accorded the broadest scope of protection in the Court's case law, including with regard to confidentiality of journalistic sources. In *Goodwin v United Kingdom*[16], the European Court of Human Rights held that:

> *"The protection of journalistic sources is one of the basic conditions for press freedom. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected. An order of source disclosure ... cannot be compatible with Article 10 unless it is justified by an overriding requirement in the public interest"*

76. The undifferentiated access to electronic communications including those between journalists and their sources constitutes a clear threat to the confidentiality of such sources.

77. Digital Rights Ireland submits that insofar as it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, the Decision has an inhibitory or "chilling" effect on freedom of expression.

78. Further, in that it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, the Decision permits the interference by public authorities with the right to receive and impart information and ideas. In this respect the Decision infringes the right to freedom of Expression as guaranteed by European Union law. Digital Rights

[16] Goodwin v United Kingdom, No 17488/90, §39, ECHR 1996

Ireland, in this regard, relies upon the finding of the Court of Justice in *Digital Rights Ireland v Ireland* as cited at paragraph 51 above.

Freedom of assembly and of association

79. The United Nations Universal Declaration of Human Rights, a source of the General Principles of European Union law, provides at Article 20.1, that

> *"Everyone has the right to freedom of peaceful assembly and association."*

80. The United Nations International Covenant on Civil and Political Rights, a source of the General Principles of European Union Law, provides at Article 22.1, that

> *"Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests. "*

81. The European Convention for the Protection of Human Rights and Fundamental Freedoms, a source of the General Principles of European Union Law, provides (*inter alia*, and subject to certain limitations) at Article 11 that

> *"Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests"*

82. The Charter of Fundamental Rights of the European Union provides at Article 12 that

> *"1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests.*
>
> *2. Political parties at Union level contribute to expressing the political will of the citizens of the Union"*

83. In *Digital Rights Ireland v Ireland*, the court held, in relation to telecommunications metadata, that

> *"Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out,* ***the social relationships of those persons and the social environments frequented by them*** (emphasis added)*"*

84. Social media data, by definition, is more than merely personal. It also relates to an individual's interaction with others, whether on an individual or group basis. Indeed, it has been seen around the world to be a tool for organisation by political and civil society groups. When such data can be accessed *en masse*, it is possible to build up a picture of entire networks of relationships. This must by necessity have implications for the right to free association, in particular where data relating to social, ethnic and political affiliations are also accessible.

85. Digital Rights Ireland further submits that by invading and thus curtailing privacy, making communications data accessible en masse by law enforcement agencies exercises a chilling effect on participation in democratic and civic activity. Without privacy, there can be no public life. If every debate is open to becoming *ad hominem*, there is no politics, no discourse of ideas at all, only a struggle for power between individuals whose ideas can never be judged solely on their own merits. Public life requires for its existence the confidence that our private lives will be kept out of it. Who will stand in the *agora* to profess or solicit support for an opinion, if they cannot be sure that they do not invite scrutiny, not of the idea, but of themselves?

86. Insofar as such monitoring amounts to surveillance of social, civil and political activity, any legislation permitting same must offend against the right to Freedom of Assembly and of Association.
87. Digital Rights Ireland therefore submits that insofar as it allows, or in the alternative, fails and has failed to safeguard against indiscriminate access by foreign law enforcement authorities to social media data, including data relating to an individual's personal relationships, family connections, civic activities and political opinions and affiliations, the Decision has an inhibitory or "chilling" effect on Freedom of assembly and of association.

Article 8.3 and Control by an Independent Authority

88. Even in the event that the data of European Citizens is not in fact being accessed on a general basis by foreign law enforcement, Digital Rights Ireland considers Article 8.3 of the Charter to be of great relevance. That provision states that compliance with Data Protection laws "shall be subject to control by an independent authority".

89. The Decision provides for no such control, and thus, irrespective of the factual situation regarding the operation of Safe Harbour, is contrary to the requirements of EU law. In this respect, it is submitted that a single Commission decision, particularly one relying on self-certification, cannot be said to provide control by an independent party, unless that decision admits of the possibility of investigation by a domestic data

protection regulator, in light of contemporary developments. It is submitted that no supervisory role played by any body outside the European Union, such as, for example, United States Federal Trade Commission can fulfil this Charter requirement for control by an independent authority.

90. Further, or in the alternative, if the Decision forbids any such further investigation by domestic data protection regulators, it cannot be said to comply with the requirements of the Charter, and must be struck down.

91. These submissions regarding Article 8.3 are made in addition to and without prejudice to those made at 28-31 above.

The Safeguards and Supervision provided for under the Decision.

92. Though largely cognate with the Data Protection Directive's requirements, the Decision and its accompanying material contains no provision for the right to object to certain kinds of processing, as provided for at Article 14 of Directive 95/46. Neither does it contain any prohibition of certain kinds of automated decision making, as does Article 15 of Directive 95/46. Further, there are no rules covering telecommunications as there are under Directive 2002/58. In this regard, the Decision can be said, on its face, to fail to adequately ensure that the European Union citizen's rights under EU law are fully provided for.

93. The Decision, in its text provides for a number of alternative means of oversight. These may be broadly divided into two categories, Enforcement and Verification. Under Annex I of the Decision, the Enforcement Principle provides that mechanisms must be in place which provide for

(a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide;

(b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented;

(c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

(a) and (c) relate to the Enforcement category, and are provided for under FAQ 11. (b) relates to the Verification category, and is provided for under FAQ 7.

Enforcement

94. Enforcement relates to the recourse offered to individuals who make complaints relating to the processing of their data under the Decision. Irrespective of the adequacy of the dispute resolutions themselves, Digital Rights Ireland submits that an enforcement model based on an obligation on the individual to initiate complaints does not provide adequate supervision of Data Protection rights as required by Article 8.1 of the Charter. It is in the nature of unauthorised processing of data that it frequently occurs on a mass basis and without the individual data subject being aware of it. Insofar as the obligation to initiate enforcement is placed on the data subject, such an enforcement model also denies the individual the right to an Effective Remedy, contrary to Article 47 of the Charter and Article 13 of the ECHR, and the right to Good Administration, contrary to Article 41 of the Charter.

95. As provided for by FAQ 11, The Enforcement options available to companies operating under Safe Harbour are as follows:

(a) compliance with private sector developed privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms of the type described in the Enforcement Principle;
(b) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or
(c) commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.

The operational adequacy of these safeguards will be considered below.

Verification

96. The Enforcement mechanisms requiring as a trigger a complaint by an individual data subject, the sole form of general oversight of the actual functioning of Safe Harbour is provided for under FAQ 7 of the Decision. That FAQ commences as follows:

> *"Q: How do organizations provide follow up procedures for verifying that the attestations and assertions they make about their safe harbor privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Safe Harbor Principles?*
>
> *A: To meet the verification requirements of the Enforcement Principle, an organization may verify such attestations and assertions either through self-assessment or outside compliance reviews."*

97. The FAQ then goes on to outline in further detail the manner in which each of these options should operate. The Portion relating to self-assessment in particular repays a close reading:

> *"Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self-assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance."*

98. It is notable that, other than the requirement, buried within the text, that the privacy policy is "completely implemented", there is little emphasis placed on the operational reality of how data is processed by companies, the stress instead falling on the adequacy of policy and documentation. More pertinantly, Digital Rights Ireland notes that a procedure whereby self-certification is followed by self-verification cannot be said to offer any true oversight, as required by Article 8.1. The Self-verification model

amounts to no more than organizations making the same assertion ("we comply with the Safe Harbour Principles") twice. By permitting such a practice in place of veritication, the Decision is in breach of the Article 8.1 requirement that supervision be independent.

99. In circumstances where organizations are offered a choice of self-certification or outside compliance review, Digital Rights Ireland does not propose to examine the adequacy of the outside compliance review model, other than to note that by reason of its being voluntary, it is *prima facie* inadequate to the requirements of Article 8.1

The Adequacy in Practice of the Safeguards Provided for in the Decisions

100. The Commission itself has raised significant concerns regarding the adequacy of oversight as provided for by the Decision. Though these concerns have not explicitly mentioned Article 8.3, it is difficult to see how any purported system of oversight could contain the flaws outlined by the Commission and yet satisfy the requirement that the Fundamental Right of European Union Citizens to Data Protection be subject to control by an independent authority

101. The Communication From the Commission To the European Parliament And the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU sets out these flaws as some considerable length. It states at Section 3:

> *"There has been a growing concern among some data protection authorities in the EU about data transfers under the current Safe Harbour scheme. Some Member States' data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by industry, referring to distortions of competition due to a lack of enforcement. The current Safe Harbour arrangement is based on the voluntary adherence of companies, on self-certification by these adhering companies and on enforcement of the self-certification commitments by public authorities. In this context any lack of transparency and any shortcomings in enforcement undermine the foundations on which the Safe Harbour scheme is constructed.*

102. Having outlined certain concerns raised by national authorities regarding the operation of Safe Harbour (inlcluding the concerns raised in the within referral), the Comminication states:

> *"These divergent responses of data protection authorities to the surveillance revelations demonstrate the real risk of the fragmentation of the Safe Harbour scheme and raise questions as to the extent to which it is enforced."*

103. Section 3 also states

> *"About 10% of companies claiming membership in the Safe Harbour are not listed by the Department of Commerce as current members of the scheme24. Such false claims originate from both: companies which have never been participants of the Safe Harbour and companies which have once joined the scheme but then failed to resubmit their self-certification to the Department of Commerce at the yearly intervals. In this case they continue to be listed on the Safe Harbour website, but with certification status "not current", meaning that the company has been a member of the scheme and thus has an obligation to continue to provide protection to data already processed. The Federal Trade Commission is competent to intervene in cases of deceptive practices and non-compliance of the Safe Harbour principles (see Section 5.1). Unclarity over the "false claims" impacts the credibility of the scheme.*
>
> *The European Commission alerted the Department of Commerce through regular contacts in 2012 and 2013 that, in order to comply with the transparency obligations, it is not sufficient for companies to only provide the Department of Commerce with a description of their privacy policy. Privacy policy statements must be made publicly available. The Department of Commerce was also asked to intensify its periodic controls of companies' websites subsequent to the verification procedure carried out in the context of the first self-certification process or its annual renewal and to take action against those companies which do not comply with the transparency requirements.*
>
> *As a first answer to EU concerns, the Department of Commerce has since March 2013 made it mandatory for a Safe Harbour company with a public website to make its privacy policy for customer/user data readily available on its public website. At the same time, the Department of Commerce began notifying all companies whose privacy policy did not already include a link to Department of Commerce Safe Harbour website that one should be added, making the official Safe Harbour List and website directly accessible to consumers visiting a company's website. This will allow European data subjects to verify immediately, without additional searches in the web, a*

company's commitments submitted to the Department of Commerce. Additionally, the Department of Commerce started notifying companies that contact information for their independent dispute resolution provider should be included in their posted privacy policy"

104. It is striking that these efforts relate solely to the *publication* of privacy policies. The question of whether the policies are *adhered* to goes unaddressed. Indeed, the Commission concedes this in its Communication:

> *"There is no full evaluation of the actual practice in the self-certified companies which would significantly increase the credibility of the self-certification process."*

105. Indeed, as outlined above, it is inherent in the Safe Harbour Decision that these questions cannot be addressed by the European Union or by any independent supervisor. The very nature of the scheme of self-certification system means that any oversight must relate largely to policies and documentation rather than to practices. For example, the process described below relates solely to the requirement that companies make the right promises, not to any requirement that they keep those promises:

> *" The Department of Commerce has assured the Commission that any certification or recertification can be finalised only if the company's privacy policy fulfils all requirements, notably that it includes an affirmative commitment to adhere to the relevant set of Safe Harbour Privacy Principles and that the privacy policy is publicly available. A company is required to identify in its Safe Harbour List record the location of the relevant policy. It is also required to clearly identify on its website an Alternative Dispute Resolution provider and include a link to the Safe Harbour self-certification on the website of the Department of Commerce."*

106. In fact, even these entirely inadequate requirements are frequently not satisfied. The Commission Communication states "*it has been estimated that over 30% of Safe Harbour members do not provide dispute resolution information in the privacy policies on their websites*". The Communication further finds that, of those companies which have been removed from the Safe Harbour List, none were removed for want of compliance.

Conclusion

107. Digital Rights Ireland submits to the Court that the Safe Harbour Decision is, and was intended to be at its conception, a final determination regarding the adequacy

of Data Protection and Privacy protections afforded by the laws and practices of the United States of America.

108. Notwithstanding that the Decision provides that certain individual data flows may, in exceptional circumstances and on a temporary basis, be halted by domestic data protection regulators, these regulators are not permitted by the Decision to reopen the question as to adequacy.

109. Insofar as the Decision thus forbids any such investigation, even in circumstances where there is reason to believe that the laws and practices of the United States of America do not provide adequate protections to the data of EU citizens, the Decision does not conform to the requirements of Article 8.3 of the Charter of Fundamental Rights.

110. Insofar as this power to suspend data flows exists in some but not all member states, the Descision, by not explicitly granting such a power to the regulators of all members states, the fails to provide equal access to a remedy to citizens across the member states of the EU, contrary to the requirements of Article 8.3 of the Charter of Fundamental Rights and in breach of the rights to an Effective Remedy and to Good Administration, as provided for under the Charter of Fundamental Rights and the General Principles of Community Law.

111. By thus permitting the creation of an irrebuttable presumption regarding the protection afforded to fundamental rights in certain third countries, the Decision undermines the safeguards provided by the Charter, in breach of the rights to an Effective Remedy and to Good Administration, as provided for under the Charter of Fundamental Rights and the General Principles of Community Law, and contrary to the general scheme and intention of the Charter of Fundamental Rights and the General Principles of Community Law.

112. In addition, insofar as the Decision allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, and fails to provide an adequate remedy to EU citizens whose personal data is thus accessed, it denies the individual the right to an Effective Remedy and the right to Good Administration, contrary to the Charter of Fundamental Rights and the General Principles of Community Law.

113. Further, insofar as the Decision allows, or in the alternative, fails and has failed to safeguard against indiscriminate access to electronic communications by foreign law enforcement authorities, it is invalid as a breach of the Rights to Privacy, Data Protection, Freedom of Expression and Freedom of Assembly and Association, as provided for under the Charter of Fundamental Rights and by the general principles of Community Law.

114. Finally, by failing to fully transpose the rights contained in Directive 95/46 (specifically at Article 14 and 15), the Decision, on its face, fails to adequately ensure that the European Union citizen's rights under EU law are fully provided for where their data is transferred to the Unites States of America.

Dated this 10th day of November, 2014.

Signed [redacted]

McGarr Solicitors

Solicitors for the Plaintiff